



FortiAnalyzer - Release Notes

VERSION 5.4.4

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



December 13, 2017

FortiAnalyzer - Release Notes

05-544-450543-20171213

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported models	6
What's new in FortiAnalyzer version 5.4.4	7
Special Notices	8
Cannot remove VDOM from the GUI	8
Hyper-V FortiAnalyzer-VM running on an AMD CPU	8
IPsec connection to FortiOS for logging	8
Datasets Related to Browse Time	8
System Configuration or VM License is Lost after Upgrade	8
SSLv3 on FortiAnalyzer-VM64-AWS	9
No support for remote SQL database	9
Pre-processing logic of ebtime	9
Log Aggregation or Forwarding	9
Naming Convention for Generated Reports	10
Upgrade Information	11
Upgrading to FortiAnalyzer 5.4.4	11
Downgrading to previous versions	11
Firmware image checksums	11
FortiAnalyzer VM firmware	11
SNMP MIB files	13
Product Integration and Support	14
FortiAnalyzer version 5.4.4 support	14
Feature support	16
FortiGate Management	16
Language support	17
Supported models	18
Resolved Issues	26
Device Manager	26
Event Management	26
FortiView	26
Log View	27
Reporting	28

System Settings	28
Others	29
Common Vulnerabilities and Exposures	29
Known Issues	30
Event Management	30
FortiView	30
Log View	30
Reports	30
Others	31

Change Log

Date	Change Description
2017-10-05	Initial release of 5.4.4.
2017-10-11	Added bugs to Resolved and Known Issues lists.
2017-10-20	Added <i>Product Integration & Support > FortiOS/FortiOS Carrier > 5.4.6.</i> Added 451717 to <i>Known Issues > Event Management.</i>
2017-10-25	Added 456270 to <i>Known Issues > Reports.</i>
2017-10-30	Added note about LENC device support.
2017-11-14	Added <i>Special Notices > Naming Convention for Generated Reports.</i>
2017-11-20	Added 2.4.0 and 2.4.1 support to <i>Product Integration & Support > FortiSandbox.</i>
2017-11-28	Added <i>Chassis Management</i> to <i>Product Integration & Support > FortiGate Management.</i>
2017-11-30	Updated <i>Upgrade Information > Upgrading to 5.4.4.</i> Users need to upgrade to at least 5.2.9 before upgrading to 5.4.4.
2017-12-13	Added FortiOS 5.4.7 support to <i>Product Integration and Support.</i>

Introduction

This document provides the following information for FortiAnalyzer version 5.4.4 build 1225:

- [Supported models](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer Upgrade Guide*.

Supported models

FortiAnalyzer version 5.4.4 supports the following models:

FortiAnalyzer	FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F, FAZ-3900E, and FAZ-4000B.
FortiAnalyzer VM	FAZ-VM64, FAZ-AWSONdemand, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).

What's new in FortiAnalyzer version 5.4.4

There are no new features or enhancements in FortiAnalyzer version 5.4.4.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 5.4.4.

Cannot remove VDOM from the GUI

A VDOM may re-appear even after it is deleted from the FortiAnalyzer GUI.

A new CLI command is introduced in FortiAnalyzer 5.4.3 to use as a workaround for this issue. You can use the following CLI command `execute log device vdom delete <Device_Name> <VDOM_Name>` to delete the VDOM from FortiAnalyzer.

Hyper-V FortiAnalyzer-VM running on an AMD CPU

A Hyper-V FAZ-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

IPsec connection to FortiOS for logging

FortiAnalyzer 5.4.2 no longer supports an IPsec connection with FortiOS 5.0/5.2. However UDP or TCP + reliable are supported.

Instead of IPsec, you can use the FortiOS reliable logging feature to encrypt logs and send them to FortiAnalyzer. You can enable the reliable logging feature on FortiOS by using the `configure log fortianalyzer setting` command. You can also control the encryption method on FortiOS by using the `set enc-algorithm default/high/low/disable` command.

FortiAnalyzer 5.4.1 and earlier does support IPsec connection with FortiOS 5.0/5.2.

Datasets Related to Browse Time

FortiAnalyzer 5.4.2 contains enhancements to calculating the estimated browse time. Due to the changes, cloned datasets that query for browse time may not be able to return any results after upgrade.

System Configuration or VM License is Lost after Upgrade

When upgrading FortiAnalyzer from 5.4.0 or 5.4.1 to 5.4.2, it is imperative to reboot the unit before installing the 5.4.2 firmware image. Please see the *FortiAnalyzer Upgrade Guide* for details about upgrading. Otherwise,

FortiAnalyzer may lose system configuration or VM license after upgrade. There are two options to recover the FortiAnalyzer unit:

1. Reconfigure the system configuration or add VM license via CLI with `execute add-vm-license <vm license>`.
2. Restore the 5.4.0 backup and upgrade to 5.4.2.

SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol tlsv1
end
```

No support for remote SQL database

Starting with FortiAnalyzer software versions 5.0.7 and 5.2.0, remote SQL database support will only cover the insertion of log data into the remote MySQL database. Historical log search and reporting capabilities, which rely on the remote SQL data, will no longer be supported.

Those wishing to use the full set of FortiAnalyzer features are encouraged to switch as soon as possible to storing SQL data locally on the FortiAnalyzer. The local database can be built based upon existing raw logs already stored on the FortiAnalyzer.

Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:

Traffic logs with `logid` of 13 or 2, when `logid == 13`, `hostname` must not be empty. The `service` field should be either HTTP, 80/TCP or 443/TCP.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.

In version 5.0.5 or later, Explicit Proxy logs (`logid=10`) are checked when calculating the estimated browsing time.

Log Aggregation or Forwarding

Log aggregation or forwarding works from 5.4 to 5.4 or 5.4.1 to 5.4.1. Please use the same FortiAnalyzer version on all the units. Other FortiAnalyzer versions not supported.

Naming Convention for Generated Reports

Starting in FortiAnalyzer 5.4.4, the file naming convention for generated reports has changed. The filename will reference the device name rather than the device ID.

Upgrade Information

Upgrading to FortiAnalyzer 5.4.4

You can upgrade FortiAnalyzer 5.2.0 or later directly to 5.4.4. If you are upgrading from versions earlier than 5.2.0, you will need to upgrade to FortiAnalyzer 5.2 first. (We recommend that you upgrade to 5.2.9, the latest version of FortiAnalyzer 5.2.)



ADOM version is not required to match the FortiGate log versions. For example, you can have FortiGate 5.4 logs in a 5.2 version ADOM.



For details about upgrading your FortiAnalyzer, see *FortiAnalyzer Upgrade Guide*.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FAZ_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FAZ_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

VMware ESX/ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtual-security-management.html>. VM installation guides are available in the [Fortinet Document Library](#).

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

Product Integration and Support

FortiAnalyzer version 5.4.4 support

The following table lists FortiAnalyzer version 5.4.4 product integration and support information:

Web Browsers	<ul style="list-style-type: none">• Microsoft Internet Explorer version 11• Mozilla Firefox version 55• Google Chrome version 61 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiOS/FortiOS Carrier	<ul style="list-style-type: none">• 5.4.0 to 5.4.7• 5.2.0 to 5.2.11• 5.0.4 to 5.0.14
FortiAnalyzer	<ul style="list-style-type: none">• 5.4.0 to 5.4.4• 5.2.0 to 5.2.11• 5.0.0 to 5.0.13
FortiCache	<ul style="list-style-type: none">• 4.2.2• 4.1.3• 4.0.4
FortiClient	<ul style="list-style-type: none">• 5.4.3• 5.2.0 and later• 5.0.4 and later
FortiMail	<ul style="list-style-type: none">• 5.3.9• 5.2.9• 5.1.6• 5.0.10
FortiManager	<ul style="list-style-type: none">• 5.4.0 to 5.4.3• 5.2.0 and later• 5.0.0 and later

FortiSandbox	<ul style="list-style-type: none">• 2.4.1• 2.4.0• 2.2.2• 2.1.3• 2.0.3• 1.4.0 and later• 1.3.0• 1.2.0 and 1.2.3
FortiSwitch ATCA	<ul style="list-style-type: none">• 5.0.0 and later• 4.3.0 and later• 4.2.0 and later
FortiWeb	<ul style="list-style-type: none">• 5.8.1• 5.8.0• 5.7.0• 5.6.0• 5.5.4• 5.4.1• 5.3.8• 5.2.4• 5.1.4• 5.0.6
FortiDDoS	<ul style="list-style-type: none">• 4.3.1• 4.2.3• 4.1.12
FortiAuthenticator	<ul style="list-style-type: none">• 4.3.2• 4.2.0
Virtualization	<ul style="list-style-type: none">• Amazon Web Service AMI, Amazon EC2, Amazon EBS• Citrix XenServer 6.2• Linux KVM Redhat 6.5• Microsoft Azure• Microsoft Hyper-V Server 2008 R2, 2012 & 2012 R2• OpenSource XenServer 4.2.5• VMware:<ul style="list-style-type: none">• ESX versions 4.0 and 4.1• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5



Always review the Release Notes of the supported platform firmware version before upgrading your device.

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer	✓		✓	
FortiCache	✓		✓	✓
FortiClient registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓	✓		✓
FortiDDoS	✓	✓	✓	✓
FortiMail	✓		✓	✓
FortiManager	✓		✓	
FortiSandbox	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	

FortiGate Management

You can enable FortiManager features on some FortiAnalyzer models. FortiAnalyzer models with FortiManager features enabled can manage a small number of FortiGate devices, and all but a few FortiManager features are enabled on FortiAnalyzer. The following table lists the supported modules for FortiAnalyzer with FortiManager Features enabled:

FortiManager Management Modules	FortiAnalyzer with FortiManager Features Enabled
Device Manager, except firmware and license management	✓
Policy & Objects	✓
AP Manager	✓
FortiClient Manager	✓
VPN Manager	✓
FortiGuard	
FortiMeter	
FGT-VM License Activation	
Chassis Management	✓

Language support

The following table lists FortiAnalyzer language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Russian		✓
Spanish		✓

To change the FortiAnalyzer language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language from the drop-down list. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <sftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information, see the *FortiAnalyzer CLI Reference*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiManager, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running version 5.4.4. Please ensure that the log devices are supported before completing the upgrade.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-61E, FG-60E-DSL, FG-60E-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-101E, FG-100EF, FG-140D, FG-140E, FG-140D-POE, FG-140E-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810D, FG-3815D, FG-2000E, FG-2500E, FG-3800D, FG-3960E, FG-3980E FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1 FortiGate 7000 Series: FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 FortiGate DC: FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC FortiGate Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC FortiWiFi: FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-30D-POE, FWF-60D, FWF-60E-DSL, FWF-60D-POE, FWF-90D, FWF-90D-POE, FWF-92D, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600D, FG-900D, FG-600C, FG-620B, FG-621B, FG-800C, FG-800D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B FortiGate 5000 Series: FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C FortiGate DC: FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FGT-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC FortiGate Low Encryption: FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC FortiWiFi: FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D FortiGate Rugged: FGR-60D, FGR-100C FortiGate VM: FG-VM-Azure, FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN FortiSwitch: FS-5203B, FCT-5902D	5.2

Model	Firmware Version
FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-700D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B FortiGate 5000 Series: FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C FortiGate DC: FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC FortiGate Low Encryption: FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC FortiWiFi: FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D FortiGate Rugged: FGR-60D, FGR-90D, FGR-100C FortiGateVoice: FGV-40D2, FGV-70D4 FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN FortiSwitch: FS-5203B	5.0

FortiCarrier Models

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C FortiCarrier DC: FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3810D-DC, FCR-3815D-DC FortiCarrier VM: FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D FortiCarrier DC: FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC FortiCarrier Low Encryption: FCR-5001A-DW-LENC FortiCarrier VM: FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-VM64-XEN, FCR-VM64-AWSONDEMAND	5.2
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C FortiCarrier DC: FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC FortiCarrier Low Encryption: FCR-5001A-DW-LENC FortiCarrier VM: FCR-VM, FCR-VM64	5.0

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B	4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. FortiAnalyzer VM: FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B FortiAnalyzer VM: FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B FortiAnalyzer VM: FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B FortiMail Low Encryption: FE-3000C-LENC FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B FortiMail VM: FE-VM64	5.1.6
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B FortiMail VM: FE-VM64	5.0.10

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-VM	2.3.2
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D FortiSandbox VM: FSA-VM	2.2.0 2.1.0
FortiSandbox: FSA-1000D, FSA-3000D FortiSandbox VM: FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-59	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-400D, FWB-600D, FWB-1000E, FWB-2000E, FWB-3010E	5.6.0
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.3

Model	Firmware Version
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.8
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FortiCache-3000E, FCH-3900E FortiCache VM: FCH-VM64, FortiCache-KVM	4.1
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E FortiCache VM: FCH-VM64	4.0

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.4.4. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
300898	IP address may be incorrect on aggregation server side after aggregation.
383872	The shown percentage of Storage Used is incorrect.
416886	FortiAnalyzer may use the FortiSandbox serial number as its hostname.
438292	There may be wrong VDOMs generated for FortiSandbox.
445742	Log status is incorrectly shown as down.
449463	The device count for Log Status Down is incorrect.

Event Management

Bug ID	Description
416552	All Events list sorting may not work.
424365	Users may not be able to have hostname in the subject of an alert email.

FortiView

Bug ID	Description
423221	IPS logs with <code>dnat</code> may not be displayed.
414263	Host name may contain user information in Endpoints.

Log View

Bug ID	Description
391882	Log Forwarding mode may change to <i>both</i> after users edit an aggregation client.
406543	There may be logs that no longer exists in the upload queue.
438189	FortiAnalyzer may send inaccurate CEF logs.
443087	Log View may display events from VDOMs managed by other ADOMs.
447011	Filter with an * asterisk may not work.
451853	FortiAnalyzer may fail to load a custom view with custom time frame.
450036	In Log Group, the device list may be empty for member selection.
450087	For AV logs in Log View, the link to FortiGuard for virus may be missing.
449890	Time period may not change when users choose Customized Time Period in Log View.
448890	Security Event list may not show UTM related events.
439740	Log Aggregation may fail because of authentication error.
437282	The page count may be inconsistent.
444061	Custom view may not work for <i>Display Raw</i> .
439350	Matching values in the <i>Source</i> column may not be highlighted in the search result.
436781	The package capture to be downloaded may miss a file type in the filename.
409314	Searching for an IP address may yield to results of searching for the individual octet of the IP address.
440103	DLP Email Archive and IPS archive packet may show each other's content.
401264	The filter criteria may not be applied if the search popup is not closed.

Reporting

Bug ID	Description
280786	There may be errors when users update chart type in <code>report char config</code> .
384890	There may be no chart output in html/pdf/sml reports when users set <code>max-table-rows</code> to 100k.
410771	FortiAnalyzer may not support the usage of device name in report titles.
415096	The dataset <code>fct-Top-Infected-Devices-with-Virus-Malware</code> may not cover both Tlog and Elog.
423343	PCI-DSS Compliance Review report may use wrong value from dataset for <i>Percent of Passed Fortinet Security Best Practices</i> .
423541	When users try to create a report from the template, the list may be empty if there is only one template.
436887	<i>Save to folder</i> feature in the rename folder page may not work.
444533	The application <code>run_rpt</code> may crash during multiple reports.
447061	Users may be unable to edit in Report Calendar.
447312	The filter may not handle commas in a username.
449787	Uploading reports in the output profile may not work.
450814	Users may not be able to specify devices in dataset.

System Settings

Bug ID	Description
297374	ADOM version may not be changed manually.
372553	In the All ADOMs page, some VDOMs may not be displayed.
406185	GB/day over usage may not display properly.
415536	Log roll may be delayed when the log roll time is set at the default 0:00.
446285	There may be no value for <i>Out of Available</i> : in the Storage Info edit page.

Bug ID	Description
448214	In the All ADOMs page, after users click on the <i>Expand</i> icon, some devices may not be displayed.
452077	A blank page may be present after reloading the System Settings page.

Others

Bug ID	Description
411825	Corrupted logs may impact rebuilding ADOM/DB.
414358	Settings <code>table-partition-time-max</code> and <code>top-dev</code> may be lost after upgrade.
443850	The <code>diagnose test app logfi 7</code> output may not be sorted.
449889	The command <code>diagnose sql upload</code> may not work.
450044	Report may not be displayed if users have two tabs of the login page in the same browser and they log in via the second tab.
451105	The application <code>fazsvcd</code> may crash when users enable FortiManager feature and disable it.

Common Vulnerabilities and Exposures

Bug ID	Description
442206	FortiAnalyzer 5.4.4 is no longer vulnerable to the following CVE-References: <ul style="list-style-type: none"> 2017-9765 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in FortiAnalyzer version 5.4.4. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Event Management

Bug ID	Description
451717	Log field values for Application Control may not match those on FortiGate.

FortiView

Bug ID	Description
452012	There might be some entries that are not WiFi Clients shown in WiFi Clients.

Log View

Bug ID	Description
451773	Log filter for USER in Event - VPN may not work.
452265	FortiAnalyzer may lose log connectivity with FortiGates under collector mode.
452287	Time frame list may be displayed incorrectly after users switch among different ADOMs.
453129	GUI may display cached information after users switch to another ADOM.

Reports

Bug ID	Description
434057	There might be unwanted characters in application category in reports.
456270	Even when no background image is set for a report, the default background image may still be used after upgrading to 5.4.4

Others

Bug ID	Description
444436	FortiAnalyzer VM interface mappings may change after a reboot.
452846	<code>Logfwd</code> may take up to 100% CPU usage when the reliable connection is enabled.
453211	Users may encounter <i>Web Server Error 500</i> in the FortiAnalyzer GUI.



FORTINET®

High Performance Network Security



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.